UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,674	11/21/2003	Joshua D. Hug	REAL-2006053	1315

61857 7590 11/23/2009

AXIOS LAW GROUP, PLLC / REALNETWORKS, INC
1525 4TH AVE, STE 800
SEATTLE, WA 98101-1648

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
11/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/719,674	HUG, JOSHUA D.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-19,31-36,38,39,41-43,45-52,54 and 56-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-19,31-36,38,39,41-43,45-52,54 and 56-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed 7-8-2009.

2. Claims **1 - 6, 8 - 19, 31 - 36, 38, 39, 41 - 43, 45 - 52, 54, 56 - 61** are pending. Claims **7, 20 - 30, 37, 40, 44, 53, 55** have been cancelled. Claims **1, 31, 34, 49** are independent. This application was filed 11-21-2003.

Response to Arguments

3. Applicant's arguments have been fully considered but were no persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, *generation of an external integrity hash and an internal integrity hash using clear forms rights information (Remarks Pages 10, 11); a hash comprising a hash of a hash in addition to a hash of a hash wherein the first and second hash both comprise the same clear form rights information (Remarks Page 14); regeneration of a hash (Remarks Page 17)*

The Hardy prior art discloses the generation of a hash consisting of a previously generated hash and an encryption key. (see Hardy col. 10, lines 56-64: combines the digest H, with signer's private key; concatenate two values; hash generated from a hash and a private encryption key) Applicant's invention discloses a second hash (external integrity hash) consisting of a previously generated hash (internal integrity hash). The cited prior art discloses an analogous structure, a hash within a hash. The clear forms rights information is disclosed as included within the initial hash and included within the resultant second hash. The Hall prior art discloses the usage of clear form rights

information plus the protection and security of data integrity using a cryptographic hash. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-28: clear form storage of digital rights information, integrity hash) Hall prior art discloses a hash of clear rights information. And, Hardy discloses a hash within a hash. Therefore, Hall and Hardy prior art combination discloses a hash of clear rights information that is integrated within another hash. It appears to the Examiner that the hash within a hash is one of the innovative concepts Applicant is attempting to patent and that the Nonaka, Hardy and Hall prior art combination disclose these claim limitations.

Regeneration of a hash is equivalent to the initial generation of a hash from a set of parameters.

3.2 Applicant argues that the referenced prior art does not disclose, *rejection of claim 1 as a whole; and/or the obviousness rejection. (Remarks Page 10)*

A 103 rejection based on multiple references is a legitimate technique according to the MPEP. The current application is rejected based on the Nonaka, Hardy, and Hall, Thoma prior art references. The set of prior art references are in a same field of endeavor as the claimed invention, generation of a hash value from a set of parameters. A 103 rejection allows portions of a claimed invention to come from different prior art references. The set of prior art references disclose the set of integrated claim limitations.

Each obviousness combination indicates the particular claim limitation the combined reference prior art teaches. In addition, a cited passage from the referenced

prior art clearly indicates the motivation for the obviousness combination. Each obviousness combination's disclosure is equivalent to Applicant's claimed limitation(s) for the claimed invention. Achieved advantage is a valid motivation for the combination of referenced prior art. The combination of each referenced prior art combination states a motivation for the combination, which translates to an achieved advantage for the combination.

Applicant is reminded that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Furthermore, in response to applicant's arguments against the reference individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

3.3 Applicant argues that the referenced prior art does not disclose, *comparison of hash to detect tampering with protected content. (Remarks Page 16, 17, 19)*

The Nonaka prior art discloses the capability to detect whether tampering has occurred but a comparison of a current hash and a base hash value. (see Nonaka paragraph [0246], lines 4-8: comparison of hash values to detect tampering) And,

Chase discloses the capability to disable content. (see Chase col. 3, lines 60-63: usage request; col. 4, lines 10-16; col. 33, lines 54-56; col. 33, lines 60-63; col. 34, lines 4-9: content compromised such as tampering, access to content disabled)

3.4 Responses for the accompanying dependent claims are the same as responses for the associated independent claims.

3.5 The Nonaka prior art discloses an apparatus for encryption functions with cryptographic key capabilities and a license (resource, device) key. (see Nonaka paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client, apparatus, license (device) key) And, the Nonaka prior art discloses an apparatus for encryption functions with cryptographic key capabilities and a license (resource, device) key. (see Nonaka paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client, apparatus, license (device) key)

The Hardy prior art discloses the generation of a hash consisting of a previously generated hash and an encryption key. (see Hardy col. 10, lines 56-64: combines the digest H, with signer's private key; concatenate two values; hash generated from a hash and a private encryption key)

In addition, the Hall prior art discloses the generation and usage of clear form rights information plus the protection and security of data integrity using a cryptographic hash. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights

management; col. 6, lines 19-28: clear form storage of digital rights information, integrity hash) And, the Thoma prior art is used to disclose and reject the inaccessible device key limitation. (see Thoma paragraph [0005], lines 1-3: content distribution; paragraph [0031], lines 15-21; paragraph [0033], lines 5-9; paragraph [0033], lines 11-12: inaccessible key)

The Nonaka prior art discloses an apparatus for encryption functions with cryptographic key capabilities and a license (resource, device) key. (see Nonaka paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client, apparatus, license (device) key) Applicant has before mentioned a unique key but the term "unique" does not appear anywhere within the specification or the original claims. There is no disclosure in the specification or the original claims that the device key is unique.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1 - 4, 8, 9, 11 - 19, 31, 34 - 36, 38, 39, 41, 42, 45 - 52, 54, 56, 57, 59, 60, 61** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Nonaka et al.** (US PGPUB No. **20030046238**) in view of **Hall et al.** (US Patent No. **7,062,500**) and further

in view of **Hardy et al.** (US Patent No. **6,079,018**) and **Thoma et al.** (US PGPUB No. **20020152393**).

Regarding Claim 1, Nonaka discloses a method comprising:

a) obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client site; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

Furthermore, Nonaka discloses:

e) storing the encrypted hash on the client device. (see Nonaka paragraph [0246], lines 1-4: storage circuit for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Furthermore, Nonaka discloses wherein obtaining an integrity hash of rights information stored at a client device; (see Nonaka paragraph [0019], lines 1-6; paragraph [0019], lines 7-11; paragraph [0027], lines 1-7: generate (i.e. obtain) integrity hash using UCP (i.e. rights) information; paragraph [0246], lines 1-4: storage circuit for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client; paragraph [0192], lines 1-5; paragraph [0239], lines 1-3: data storage)

Nonaka does not specifically disclose whereby rights information stored in a clear form.

However, Hall discloses:

b) obtaining a clear form external integrity hash of first data comprising said clear form rights information; c) obtaining an internal hash of second data comprising said clear form rights information; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key.

However, Hardy discloses wherein a hash comprising said clear form rights information and an external key as an integrity secret. (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a previous hash and a private encryption key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall for a hash comprising said clear form rights information and an external key as

taught by Hardy. One of ordinary skill in the art would have been motivated to employ the teachings of Hardy for a technique that can reliably generate a highly unguessable pseudo-random KEY seed value for use in a digital signature procedure such as DSA. (see Hardy col. 7, lines 54-57)

Furthermore, Nonaka-Hall-Hardy discloses wherein encrypting the integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device; (see Nonaka paragraph [0026], lines 21-25: encryption utilized UCP (i.e. rights) information; paragraph [0036], lines 1-4: license (i.e. device) keys utilized; paragraph [0346], lines 5-8)

Nonaka-Hall-Hardy does not specifically disclose whereby a device key being externally inaccessible from the client device.

However, Thoma discloses:

c) device key being externally inaccessible from the client device; (see Thoma paragraph [0005], lines 1-3: content distribution; paragraph [0031], lines 15-21; paragraph [0033], lines 5-9; paragraph [0033], lines 11-12: inaccessible key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall-Hardy for an inaccessible key as taught by Thoma. One of ordinary skill in the art would have been motivated to employ the teachings of Thoma for selection of a terminal device to receive, distribute digital content from a wide variety of devices. (see Thoma paragraph [0012], lines 7-13)

Regarding Claims 2, 35, 50, Nonaka discloses the method, client device, machine readable medium of claims 1, 34, 49, wherein obtaining the clear form external integrity hash comprises: receiving the clear form external integrity hash from a server device. (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: receive hash, UCP (i.e. rights) information; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, server)

Regarding Claims 3, 36, 51, Nonaka discloses the method, client device, machine readable medium of claims 1, 34, 49, wherein obtaining the internal integrity hash comprises: generating the internal integrity hash on the client device. (see Nonaka paragraph [0027], lines 1-7: generate hash; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Regarding Claims 4, 52, Nonaka discloses the method, machine readable medium of claims 1, 49.

Nonaka does not specifically disclose storing the rights information on the client device in a clear form

However, Hall discloses comprising storing said clear form external integrity hash on the client device. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for

the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Regarding Claims 8, 56, Nonaka discloses the method, machine readable medium of claims 1, 49, further comprising:

a) receiving, at the client device, a content key for the content; (see Nonaka paragraph [0026], lines 21-25: receive encryption key)

Furthermore, Nonaka discloses the following:

b) encrypting the content key using the client device key to generate an encrypted content key; (see Nonaka paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized) and

c) storing the encrypted content key on the client device. (see Nonaka paragraph [0246], lines 1-4: storage circuit for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Regarding Claims 9, 42, 57, Nonaka discloses the method, client device, machine readable medium of claims 1, 34, 49 further comprising:

a) generating a validation hash from at least the rights information; (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing

apparatus (i.e. client device); paragraph [0027], lines 1-7: generate integrity (i.e. validation) hash)

Furthermore, Nonaka discloses the following:

b) decrypting the encrypted internal integrity hash to recover the internal integrity hash; (see Nonaka paragraph [0019], lines 1-6; paragraph [0021], lines 3-8: decryption of UCP (i.e. rights) information) and

c) comparing the validation hash to the integrity hash to detect tampering with the rights information. (see Nonaka paragraph [0246], lines 4-8: comparison of hash values to detect tampering)

Regarding Claim 11, Nonaka discloses the method of claim 1. (see Nonaka paragraph [0246], lines 1-4: storage circuit for UCP (i.e. rights information), and content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Nonaka does not specifically disclose storing the rights information on the client device in a clear form.

However, Hall discloses wherein storing the rights information on the client device in a clear form. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall in order to

ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Regarding Claims 12, 60, Nonaka discloses the method, machine readable medium of claims 10, 59, further comprising: reading the clear form rights information from the client device out to a server device. (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: transfer UCP (i.e. rights) information)

Nonaka does not specifically disclose whereby reading the rights information from the client device in the clear form.

However, Hall discloses wherein reading the rights information from the client device. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for reading the rights information from the client device in the clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall in order to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Regarding Claims 13, 61, Nonaka discloses the method, machine readable medium of claims 1, 49, wherein the clear form rights information comprises usage information, the method further comprising:

a) tracking usage of the content; (see Nonaka paragraph [0053], lines 23-27: track

content usage)

Furthermore, Nonaka discloses the following:

b) updating the clear form rights information with changes in usage; (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: transfer (i.e. update) UCP (i.e. rights) information)

for each update of the clear form rights information;

d) re-encrypting, and re-storing the internal integrity hash on the client device. (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing apparatus (i.e. client device); paragraph [0027], lines 1-7: re-generate (i.e. generate a second time) integrity hash; paragraph [0246], lines 1-4: storage circuit for encrypted UCP (i.e. rights) information)

Nonaka does not specifically disclose a hash of second data comprising a hash and a key.

However, Hall discloses:

c) re-obtaining the internal integrity hash of second data comprising the updated clear form rights information; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital

rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key.

However, Hardy discloses wherein the hash of second data comprising said clear form external integrity hash, and said externally inaccessible client device key. (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a hash and a private encryption key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall for a hash comprising said clear form rights information and an external key as an integrity secret as taught by Hardy. One of ordinary skill in the art would have been motivated to employ the teachings of Hardy for a technique that can reliably generate a highly unguessable pseudo-random KEY seed value for use in a digital signature procedure such as DSA. (see Hardy col. 7, lines 54-57)

Regarding Claim 14, Nonaka discloses the method of claim 1 wherein the internal integrity hash comprises a Hash Message Authentication Code (HMAC). (see Nonaka paragraph [0027], lines 1-7: generate a hash (i.e. integrity hash) value utilizing cryptographic (i.e. encryption/decryption key) procedures in a hash authentication processing system)

Regarding Claims 15, 46, Nonaka discloses the method, client device of claims 1, 34,

wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path. (see Nonaka paragraph [0036], lines 1-4: license (i.e. device) key utilized; paragraph [0346], lines 5-8: inaccessible secure device utilized for hash generation)

Regarding Claim 16, Nonaka discloses the method of claim 1 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone. (see Nonaka paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client device such as a PDA, cellular phone, or MP3 player (i.e. systems containing CPU))

Regarding Claim 17, Nonaka discloses the method of claim 1 further comprising at least one of:

a) downloading the clear form rights information from a server device; (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: transfer (i.e. download) UCP (i.e. rights) information) and

Furthermore, Nonaka discloses:

b) installing a storage medium having the rights information stored thereon. (see Nonaka paragraph [0537], lines 3-6: place (i.e. install) on recording medium containing UCP (i.e. rights) information)

Regarding Claim 18, Nonaka discloses the method of claim 1 wherein the clear form

rights information grants unlimited play for the content on the client device. (see Nonaka paragraph [0339], lines 2-6: playback module; paragraph [0346], lines 1-5: playback content data)

Regarding Claim 19, Nonaka discloses the method of claim 3 wherein generating the internal integrity hash comprises generating the integrity hash in trusted hardware. (see Nonaka paragraph [0027], lines 1-7: obtain, generate integrity hash: SAM (i.e. trusted, secure hardware), generate hash; paragraph [0346], lines 5-8: inaccessible secure, trusted device)

Regarding Claim 31, Nonaka discloses a method comprising:

a) generating a validation hash from validation data comprising stored clear form rights information associated with content stored on a client device; (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing apparatus (i.e. client device); paragraph [0027], lines 1-7: generate integrity hash; paragraph [0192], lines 1-5; paragraph [0239], lines 1-3: data may be stored in an unencrypted (clear text) form)

Furthermore, Nonaka discloses:

c) comparing the validation hash to the integrity hash to detect tampering with the clear form rights information. (see Nonaka paragraph [0246], lines 4-8: comparison hash values to detect tampering)

Furthermore, Nonaka discloses wherein decrypting an encrypted hash to recover an

integrity hash using an externally inaccessible device key client device key, said integrity hash having been previously generated from data comprising the stored rights information and a clear form hash of at least the clear form rights information; (see Nonaka paragraph [0019], lines 1-6; paragraph [0021], lines 3-8: decryption UCP (i.e. rights) information; paragraph [0346], lines 5-8: inaccessible secure device utilized for hash generation; paragraph [0192], lines 1-5; paragraph [0239], lines 1-3: data storage)

Nonaka does not specifically disclose whereby stored clear form rights information. However, Hall discloses:

b) stored clear form rights information; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does not specifically disclose a client device key that is externally inaccessible.

However, Thoma discloses wherein a client device key that is externally inaccessible from the client device. (see Thoma paragraph [0005], lines 1-3: content distribution;

paragraph [0031], lines 15-21; paragraph [0033], lines 5-9; paragraph [0033], lines 11-12: inaccessible key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall for an inaccessible key as taught by Thoma. One of ordinary skill in the art would have been motivated to employ the teachings of Thoma for selection of the terminal device to receive, distribute digital content from a wide variety of devices. (see Thoma paragraph [0012], lines 7-13)

Regarding Claim 34, Nonaka discloses a client device comprising:

d) encryption circuitry to encrypt the integrity hash using the client device key to generate an encrypted hash; (see Nonaka paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized)

Furthermore, Nonaka discloses:

e) said memory being further operative to store the encrypted hash. (see Nonaka paragraph [0246], lines 1-4: storage circuit for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Furthermore, Nonaka discloses wherein a memory operative to store content and rights information associated with the content, said memory being externally accessible; (see Nonaka paragraph [0246], lines 1-4: storage circuit for content key data; paragraph [0192], lines 1-5; paragraph [0239], lines 1-3: data storage) And, Nonaka discloses wherein hash circuitry operative to obtain an external integrity

hash of first data comprising rights information; (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing apparatus (i.e. client device); paragraph [0027], lines 1-7: generate (i.e. obtain) integrity hash)

Nonaka does not specifically disclose whereby to store clear form rights information and a second integrity hash.

However, Hall discloses:

b); c); d) to store clear form rights information; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key.

However, Hardy discloses:

d) obtain an internal integrity hash of second data comprising information, the external integrity hash, and the client device key; (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a hash and a private encryption

key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall for a hash comprising said rights information and an external key as an integrity secret as taught by Hardy. One of ordinary skill in the art would have been motivated to employ the teachings of Hardy for a technique that can reliably generate a highly unguessable pseudo-random KKEY seed value for use in a digital signature procedure such as DSA. (see Hardy col. 7, lines 54-57)

Furthermore, Nonaka-Hall-Hardy discloses wherein a register to store a client device key. (see Nonaka paragraph [0048], lines 1-4: register usage by data processing apparatus)

Nonaka-Hall does not specifically disclose an externally inaccessible key.

However, Thoma discloses:

a) said register operative for storing a client device key being externally inaccessible from the client device; (see Thoma paragraph [0005], lines 1-3: content distribution; paragraph [0031], lines 15-21; paragraph [0033], lines 5-9; paragraph [0033], lines 11-12: inaccessible key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall-Hardy for an inaccessible key as taught by Thoma. One of ordinary skill in the art would have been motivated to employ the teachings of Thoma for selection of the terminal device to receive, distribute digital content from a wide variety of devices. (see Thoma paragraph [0012], lines 7-13)

Regarding Claim 38, Nonaka discloses the client device of claim 34, said memory being further operative to store the integrity hash. (see Nonaka paragraph [0246], lines 1-4: storage circuit for content data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Nonaka does not specifically disclose whereby to store the clear form external integrity hash.

However, Hall discloses wherein to store the second integrity hash in a clear form. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information (integrity hash) in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Regarding Claims 39, 54, Nonaka discloses the method, machine readable medium of claims 35, 50, wherein the external key comprises a server device key (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: receive hash, UCP (i.e. rights) information; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, server), said server device having generated the second integrity hash using a server device key. (see Nonaka

paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, server)

Regarding Claim 41, Nonaka discloses the client device of claim 34 wherein

a) the encryption circuitry further operative is to encrypt a content key for the content using the client device key; (see Nonaka paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized)

Furthermore, Nonaka discloses:

b) the memory is further operative to store the encrypted content key on the client device. ((see Nonaka paragraph [0246], lines 1-4: storage circuit (i.e. memory) for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client))

Regarding Claim 45, Nonaka discloses the method of claim 1 wherein the rights information comprises usage information, the client device further comprising::

a) tracking circuitry to track usage of the content and update the clear form rights information with changes in usage; (see Nonaka paragraph [0053], lines 23-27: track content usage; paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: transfer (i.e. update) UCP (i.e. rights) information)

Furthermore, Nonaka discloses:

b) wherein the hash circuitry and the encryption circuitry are further operative to regenerate, re-encrypting, and re-storing the internal integrity hash on the client device. (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing apparatus (i.e. client device); paragraph [0027], lines 1-7: re-generate (i.e. generate a second time) integrity hash; paragraph [0246], lines 1-4: storage circuit for encrypted UCP (i.e. rights) information)

Nonaka does not specifically disclose rights information stored in a clear form. However, Hall discloses wherein clear form rights information. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nanaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Regarding Claim 47, Nonaka discloses the client device of claim 34 further comprising at least one of:

a) an input port to download the clear form rights information from a server device; (see Nonaka paragraph [0019], lines 7-10: interface (i.e. bus) for UCP (i.e. rights) information transfer) and

Furthermore, Nonaka discloses:

b) a storage medium port to receive a storage medium having the clear form rights information stored thereon. (see Nonaka paragraph [0246], lines 1-4: storage circuit for UCP (i.e. rights) information)

Regarding Claim 48, Nonaka discloses the client device of claim 47 wherein the memory at least partially comprises the storage medium. (see Nonaka paragraph [0246], lines 1-4: storage circuit (i.e. memory) for content data)

Regarding Claim 49, Nonaka discloses a machine readable medium having stored thereon machine executable instructions, the execution of which to implement a method comprising:

c) obtaining an integrity hash of the rights information; (see Nonaka paragraph [0019, lines 1-6; paragraph [0019], lines 7-11: data processing apparatus (i.e. client device); paragraph [0027], lines 1-7: generate (i.e. obtain) integrity hash)

Furthermore, Nonaka discloses the following:

e) encrypting the integrity hash using the client device key to generate an encrypted hash; (see Nonaka paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized) and

f) storing the encrypted hash on the client device. (see Nonaka paragraph [0246], lines 1-4: storage circuit for encrypted content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Furthermore, Nonaka disclose wherein receiving rights information at a client device, said rights information being associated with content stored on the client device, said client device having a client device key and storing the rights information on the client device. (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: transfer UCP (i.e. rights) information; paragraph [0346], lines 5-8: inaccessible secure device utilized for hash generation; paragraph [0192], lines 1-5; paragraph [0239], lines 1-3: data storage)

Nonaka does not specifically disclose whereby receiving clear form rights information, and storing the rights information in a clear form.

However, Hall discloses the following:

a) receiving clear form rights information, (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

b) storing the rights information in a clear form; (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

d) obtaining an internal integrity hash of second data comprising said clear form rights information. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka

for the receipt and storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key.

However, Hardy discloses wherein a second hash comprising a integrity hash and a client device key. (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a hash and a private encryption key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall for a hash comprising said clear form rights information and an external key as an integrity secret as taught by Hardy. One of ordinary skill in the art would have been motivated to employ the teachings of Hardy for a technique that can reliably generate a highly unguessable pseudo-random KKEY seed value for use in a digital signature procedure such as DSA. (see Hardy col. 7, lines 54-57)

Nonaka-Hall-Hardy does not specifically disclose a client device key that is externally inaccessible.

However, Thoma discloses wherein a client device key that is externally inaccessible from the client device. (see Thoma paragraph [0005], lines 1-3: content distribution; paragraph [0031], lines 15-21; paragraph [0033], lines 5-9; paragraph [0033], lines

11-12: inaccessible key)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall-Hardy for an inaccessible key as taught by Thoma. One of ordinary skill in the art would have been motivated to employ the teachings of Thoma for selection of a terminal device to receive, distribute digital content from a wide variety of devices. (see Thoma paragraph [0012], lines 7-13)

Regarding Claim 59, Nonaka discloses the method of claim 49 wherein the rights information grants unlimited play for the content on the client device. (see Nonaka paragraph [0246], lines 1-4: storage circuit for UCP (i.e. rights information), and content key data; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client; paragraph [0362], lines 1-2; paragraph [0477], lines 1-3: unrestricted (unlimited) playback)

6. Claims **5, 6** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Nonaka-Hall-Hardy-Thoma** and further in view of **Serret-Avila et al.** (US Patent No. **6,959,384**).

Regarding Claim 5, Nonaka discloses the method of claim 1 further comprising receiving the external key at the client device

storing the integrity hash on the client device. (see Nonaka paragraph [0246], lines 1-4: storage circuit for content key data (i.e. first or second integrity hash); paragraph

[0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, client)

Nonaka does not specifically disclose storing the integrity hash in a clear form. However, Hall discloses:

b) storing the integrity hash in a clear form. (see Hall col. 2, lines 7-14; col. 6, lines 12-16; col. 6, lines 28-32: digital rights management; col. 6, lines 19-22: clear form storage of digital rights information)

It would have been obvious to one of ordinary skill in the art to modify Nonaka for the storage of digital rights information in clear form as taught by Hall. One of ordinary skill in the art would have been motivated to employ the teachings of Hall to ensure data structure integrity, flexibility, interoperability in the management of digital rights information. (see Hall col. 1, lines 34-37)

Nonaka-Hall does specifically disclose the capability to generate a second integrity hash using a first integrity hash.

However, Serret-Avila discloses:

a) obtaining a second integrity hash of the rights information; (see Serret-Avila col.4, lines 43-49; col. 5, lines 2-11: integrity hash generation using input hash value)

It would have been obvious to one of ordinary skill in the art to modify Nonaka-Hall to generate a second integrity hash as taught by Serret-Avila. One of ordinary skill in the art would have been motivated to employ the teachings of Serret-Avila for a relatively fast, secure, and efficient authentication of data streams. (see Serret-

Avila col. 2, line 66 - col. 3, line 3)

Regarding Claim 6, Nonaka discloses the method of claim 5 wherein obtaining the second integrity hash comprises: receiving the second integrity hash from a server device (see Nonaka paragraph [0476], lines 1-4; paragraph [0525], lines 3-6: receive hash, UCP (i.e. rights) information; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, server), said server device having generated the second integrity hash using a server device key. (see Nonaka paragraph [0026], lines 21-25: encryption utilized; paragraph [0036], lines 1-4: license (i.e. device) key utilized; paragraph [0019], lines 1-6; paragraph [0019], lines 7-11: data processing apparatus; paragraph [0339], lines 2-6: attached host CPU, server)

7. Claims **10, 32, 33, 43, 58** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Nonaka-Hall-Hardy-Thoma** and further in view of **Chase, Jr et al.** (US Patent No. **7,080,043**).

Regarding Claims 10, 32, 43, 58, Nonaka discloses the method of claim 9. (see Nonaka paragraph [0246], lines 4-8: comparison of hash values to detect tampering) Nonaka does not specifically disclose disabling content.
However, Chase discloses wherein disabling the content on the client device if tampering is detected. (see Chase col. 3, lines 60-63: usage request; col. 4, lines 10-16;

col. 33, lines 54-56; col. 33, lines 60-63; col. 34, lines 4-9: content compromised such as tampering, access to content disabled)

It would have been obvious to one of ordinary skill in the art to modify Nonaka to disable access to content as taught by Chase. One of ordinary skill in the art would have been motivated to employ the teachings of Chase to efficiently manage the rights attached to digital data such as the capability to revoke content if compromised, and add or remove a particular right. (see Chase col. 2, lines 47-51)

Regarding Claim 33, Nonaka discloses the method of claim 31 further comprising: wherein to initiate generation of the validation hash and comparison to the integrity hash. (see Nonaka paragraph [0027], lines 1-7: generation of validation hash; paragraph [0246], lines 4-8: comparison hash values to detect tampering).

Nonaka does not specifically disclose the capability to disable content.

However, Chase discloses the following:

a) receiving a usage request for the content stored at the client device, said usage request; (see Chase col. 3, lines 60-63: usage request; col. 4, lines 10-16; col. 33, lines 54-56; col. 33, lines 60-63; col. 34, lines 4-9: content compromised, access to content disabled) and

b) permitting usage only if the content is not disabled. (see Chase col. 4, lines 10-16; col. 33, lines 54-56; col. 33, lines 60-63; col. 34, lines 4-9: content compromised, access to content disabled)

It would have been obvious to one of ordinary skill in the art to modify Nonaka

to disable content as taught by Chase. One of ordinary skill in the art would have been motivated to employ the teachings of Chase to efficiently manage the rights attached to digital data such as the capability to revoke content if compromised, and add or remove a particular right. (see Chase col. 2, lines 47-51)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton Johnson whose telephone number is 571-270-1032. The examiner can normally be reached Monday through Friday from 8:00AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
November 9, 2009